

0941.63996

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application )

Applicant: Sasaki et al. )

Serial No. )

Filed: April 27, 2000 )

For: FILE PROCESSING UNIT )

Art Unit: )

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Asst. Comm. for Patents, Washington, D.C. 20231, on this date.

04-27-00  
Date

Express Mail Label No.: EL409492192US

CLAIM FOR PRIORITY

Assistant Commissioner for Patents  
Washington, DC 20231

Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 11-125010

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns  
Registration No. 29, 367

April 27, 2000  
Suite 8660 - Sears Tower  
233 S. Wacker Drive  
Chicago, Illinois 60606-6501  
Telephone: (312) 993-0080  
Facsimile: (312) 993-0633

D. John H. Sullivan  
8-10-00

#2 PATENT

10525 U.S. PTO  
09/559138



日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

1c525 U.S. PTO  
09/559138  
04/27/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application:

1999年 4月30日

出願番号  
Application Number:

平成11年特許願第125010号

出願人  
Applicant(s):

富士通株式会社

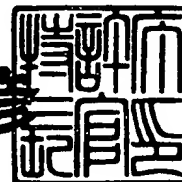
CERTIFIED COPY OF  
PRIORITY DOCUMENT

BEST AVAILABLE COPY

2000年 1月14日

特許庁長官  
Commissioner,  
Patent Office

近藤隆彦



出願受理 出願特許 11 - 2004227

PATENT OFFICE  
JAPANESE GOVERNMENT



This is to certify that the annexed is a true copy  
of the following application as filed with this office.

Date of Application: April 30, 1999

Application Number: Japanese Patent Application  
No. 11-125010

Applicant(s) FUJITSU LIMITED

January 14, 2000

Commissioner,  
Patent Office

Takahiko Kondo (Seal)

Certificate No.11-3094227

【書類名】 特許願

【整理番号】 9900476

【提出日】 平成11年 4月30日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 G06F 13/00

【発明の名称】 ファイル処理ユニット

【請求項の数】 17

【発明者】

    【住所又は居所】 東京都港区芝浦四丁目 1 5 番 3 3 号 株式会社富士通ビ  
                                 ー・エス・シー内

    【氏名】 佐々木 孝興

【発明者】

    【住所又は居所】 東京都港区芝浦四丁目 1 5 番 3 3 号 株式会社富士通ビ  
                                 ー・エス・シー内

    【氏名】 波多野 武

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通  
                                 株式会社内

    【氏名】 秋山 良太

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通  
                                 株式会社内

    【氏名】 小谷 誠剛

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通  
                                 株式会社内

    【氏名】 長谷部 高行

【特許出願人】

    【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100070150

【郵便番号】 150

【住所又は居所】 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデン  
プレイスタワー32階

【弁理士】

【氏名又は名称】 伊東 忠彦

【電話番号】 03-5424-2511

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704678

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ファイル処理ユニット

【特許請求の範囲】

【請求項 1】 コンピュータシステム内で動作するアプリケーションにて使用されたファイルのクローズ要求が発せられたときに、そのクローズ要求に応答し、当該ファイルのデータを用いて所定の規則に従って第一の署名情報を作成する第一の署名情報作成手段と、

該第一の署名情報をクローズ要求に係るファイルと関連付けて記憶装置内に格納する署名情報格納制御手段とを備えるファイル処理ユニット。

【請求項 2】 請求項 1 記載のファイル処理ユニットにおいて、

上記第一の署名情報作成手段は、クローズ要求に従って当該ファイルが記憶装置に格納された後に、該ファイルのデータを記憶装置から読み出すクローズファイル読み出し手段を有し、該クローズファイル読み出し手段にて読み出されたデータを用いて第一の署名情報を作成するようにしたファイル処理ユニット。

【請求項 3】 請求項 1 または 2 記載のファイル処理ユニットにおいて、

署名情報格納制御手段は、クローズ要求に係るファイルに第一の署名情報を付加する署名情報付加手段を有し、当該クローズ要求に係るファイルと第一の署名情報を一体的に記憶装置に格納するようにしたファイル処理ユニット。

【請求項 4】 請求項 1 乃至 3 いずれか記載のファイル処理ユニットにおいて

上記クローズ要求時にクローズ要求に係るファイルに署名情報を付加すべきか否かを判定する署名付加判定手段を有し、

当該クローズ要求に係るファイルに署名情報を付加すべきであると署名付加判定手段が判定したときに、上記第一の署名情報作成手段が第一の署名情報を作成するようにしたファイル処理ユニット。

【請求項 5】 請求項 4 記載のファイル処理ユニットにおいて、

アプリケーションにてファイルが使用される前に、少なくともクローズ要求に係るファイルに署名情報を付加する処理モードの設定を行うモード設定手段を有し、

上記署名付加判定手段は、予め設定された処理モードに基づいて当該クローズ要求に係るファイルに署名情報を付加すべきか否かを判定するモード判定手段を有するファイル処理ユニット。

【請求項 6】請求項 1 乃至 5 いずれか記載のファイル処理ユニットにおいて

上記アプリケーションで使用すべきファイルのオープン要求が発せられたときに、そのオープン要求に応答して、当該ファイルのデータを用いて上記所定の規則に従って第二の署名情報を作成する第二の署名情報作成手段と、

オープン要求に係るファイルに関連付けられて上記記憶装置内に格納された第一の署名情報と上記第二の署名情報とが一致するか否かを判定する署名一致判定手段と、

アプリケーションに提供すべき上記署名一致判定手段での判定結果を表す情報を作成する判定結果作成手段とを有するファイル処理ユニット。

【請求項 7】請求項 6 記載のファイル処理ユニットにおいて、

上記第二の署名情報作成手段は、オープン要求に係る処理が完了する前に、オープン要求に係るファイルのデータを記憶装置から読み出すオープンファイル読み出し手段を有し、該オープンファイル読み出し手段にて読み出されたデータを用いて第二の署名情報を作成するようにしたファイル処理ユニット。

【請求項 8】請求項 6 または 7 記載のファイル処理ユニットにおいて、

上記オープン要求時にオープン要求に係るファイルに対応付けられて記憶装置内に格納された第一の署名情報のチェックを行うべきか否かを判定する署名チェック判定手段を有し、

当該オープン要求に係るファイルに対応付けられて記憶装置内に格納された第一の署名情報のチェックを行うべきであると署名チェック判定手段が判定したときに、上記第二の署名情報作成手段が上記第一の署名情報との一致を判定すべき第二の署名情報を作成するようにしたファイル処理ユニット。

【請求項 9】請求項 8 記載のファイル処理ユニットにおいて、

上記署名チェック判定手段は、アプリケーションにてファイルが使用される前に、少なくともオープン要求に係るファイルに関連付けて記憶装置に格納された第

一の署名情報のチェックを行う処理モードの設定を行うモード設定手段を有し、  
上記署名チェック判定手段は、予め設定された処理モードに基づいて当該オープン要求に係るファイルに関連づけて記憶層内に格納された第一の署名情報のチェックを行うべきか否かを判定するモード判定手段を有するファイル処理ユニット。

【請求項 10】 コンピュータシステム内で動作するアプリケーションにて使用すべきファイルのオープン要求が発せられたときに、そのオープン要求に応答して、当該ファイルのデータを用いて所定の規則に従って第二の署名情報を作成する第二の署名情報作成手段と、

オープン要求に係るファイルのデータを用いて予め上記所定の規則に従って作成され、該ファイルに関連付けられて記憶装置内に格納された第一の署名情報と上記第二の署名情報とが一致するか否かを判定する署名一致判定手段と、

アプリケーションに提供すべき上記署名一致判定手段での判定結果を表す情報を作成する判定結果作成手段とを有するファイル処理ユニット。

【請求項 11】 請求項 10 記載のファイル処理ユニットにおいて、

上記第二の署名情報作成手段は、オープン要求に係る処理が完了する前に、オープン要求に係るファイルのデータを記憶装置から読み出すオープンファイル読み出し手段を有し、該オープンファイル読み出し手段にて読み出されたデータを用いて第二の署名情報を作成するようにしたファイル処理ユニット。

【請求項 12】 請求項 10 または 11 記載のファイル処理ユニットにおいて

上記オープン要求時にオープン要求に係るファイルに対応付けられて記憶装置内に格納された第一の署名情報のチェックを行うべきか否かを判定する署名チェック判定手段を有し、

当該オープン要求に係るファイルに対応付けられて記憶装置内に格納された第一の署名情報のチェックを行うべきであると署名チェック判定手段が判定したときに、上記第二の署名情報作成手段が上記第一の署名情報との一致を判定すべき第二の署名情報を作成するようにしたファイル処理ユニット。

【請求項 13】 請求項 12 記載のファイル処理ユニットにおいて、



上記署名チェック判定手段は、アプリケーションにてファイルが使用される前に、少なくともオープン要求に係るファイルに関連付けて記憶装置に格納された第一の署名情報のチェックを行う処理モードの設定を行うモード設定手段を有し、

上記署名チェック判定手段は、予め設定された処理モードに基づいて当該オープン要求に係るファイルに関連づけて記憶装置に格納された第一の署名情報のチェックを行うべきか否かを判定するモード判定手段を有するファイル処理ユニット。

【請求項 14】 アプリケーションからのイベントに基づいてファイルに対する処理を実行するファイルシステムを有するコンピュータシステムに適用されるファイル処理ユニットにおいて、

アプリケーションからのファイルクローズのイベントに係るファイルに対するファイルシステムでの処理が完了する前に、該ファイルクローズのイベントを受け取りそのイベントに係るファイルのデータを用いて所定の規則に従って第一の署名情報を作成する第一の署名情報作成手段と、

該第一の署名情報を上記ファイルクローズのイベントに係るファイルに関連付けて記憶装置に格納する署名情報格納制御手段と、

上記第一の署名情報が作成された後に、上記ファイルクローズのイベントに係るファイルに対する上記ファイルシステムでの処理への復帰処理を行う第一の復帰手段とを備えたファイル処理ユニット。

【請求項 15】 アプリケーションからのイベントに基づいてファイルに対する処理を実行するファイルシステムを有するコンピュータシステムに適用されるファイル処理ユニットにおいて、

アプリケーションからのファイルクオープンのイベントに係るファイルに対するファイルシステムでの処理が完了する前に、該ファイルクオープンのイベントを受け取りそのイベントに係るファイルのデータを用いて所定の規則に従って第二の署名情報を作成する第二の署名情報作成手段と、

オープン要求に係るファイルのデータを用いて予め上記所定の規則に従って作成され、該ファイルに関連付けられて記憶装置内に格納された第一の署名情報と上記第二の署名情報とが一致するか否かを判定する署名一致判定手段と、

アプリケーションに提供すべき上記署名一致判定手段での判定結果を表す情報を作成する判定結果作成手段と、

上記判定結果を表す情報が作成された後に、上記判定結果を表す情報をファイルシステムに渡すと共に、上記ファイルオープンのイベントに係るファイルに対する上記ファイルシステムでの処理への復帰処理を行う第二の復帰手段とを備えたファイル処理ユニット。

【請求項 16】当該コンピュータシステムに接続される外部ユニットとして構成される請求項 1 乃至 15 いずれか記載のファイル処理ユニット。

【請求項 17】上記外部ユニットが PC カードとなる請求項 16 記載のファイル処理ユニット。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ファイルオープン、ファイルクローズ、リード、ライト等のアプリケーションからの外部記憶装置に対するファイルアクセスに基づいて処理を行うファイル処理ユニットに係り、詳しくは、指定されたファイルに対する署名の作成及び署名のチェックを行うファイル処理ユニットに関する。

【0002】

【従来の技術】

コンピュータシステムを用いて作成され、外部記憶装置（ハードディスク、光ディスク、フロッピーディスク等）に格納されたファイルのデータが他人によって改ざんされたか否かを判定するために、作成されたファイルの全部または一部を用いて作成された署名データがファイルに添付される。このような署名データの作成、チェックについては、従来、専用アプリケーションによってなされている。具体的には、次のような手順にて署名データの作成、チェックが行われる。

【0003】

所望のアプリケーションによって作成されたファイルは外部記憶装置に格納される。その後、専用アプリケーションが立ち上げられ、その専用アプリケーションに従って作成されたファイルが外部記憶装置から読み出され、その読み出され

たファイルの全部または一部のデータを用いて署名データが作成される。そして、この作成された署名データが対応するファイルに添付された状態で当該ファイルが再び外部記憶装置に格納される。

【0004】

また、所望のアプリケーションによって外部記憶装置に格納されたファイルのデータの編集を行う場合、当該所望のアプリケーションが処理の対象となるファイルをアクセスする前に、専用アプリケーションが立ち上げられる。この専用アプリケーションに従って、処理の対象となるファイルのデータが外部記憶装置から読み出され、そのデータの全部または一部を用いて署名データが作成される。そして、この作成された署名データと、当該ファイルに既に添付された署名データとが比較され、それらが一致する場合には、適正なファイルのデータであるとして判定される。一方、上記両署名データが一致しない場合、当該処理の対象となるファイルのデータが前回署名データが作成されたときから現在に至る間に改ざんされたと判定される。

【0005】

ユーザは、上記のような署名データのチェックの結果に基づいて、処理対象となるファイルのデータが改ざんされたか否かを認識できる。その後、所望のアプリケーションが処理の対象となるファイルのデータを外部記憶装置から読み出して、編集等の処理が実行される。

【0006】

【発明が解決しようとする課題】

上記のように専用アプリケーションによって署名データの作成、チェックを行うようにした従来のシステムでは、所望のアプリケーションによってファイルに対する処理を実行する前に、常に、専用アプリケーションを立ち上げて署名データの作成、チェックを行わなければならない。そのため、その操作が煩雑になってしまう。

【0007】

そこで、本発明の課題は、所望のアプリケーションにて外部記憶装置に格納されたファイルをアクセスする際に、簡単に署名情報の作成、チェックが行えるよ

うなファイル処理システムを提供することる。

【0008】

【課題を解決するための手段】

上記課題を解決するため、本発明に係るファイル処理ユニットは、請求項1に記載されるように、コンピュータシステム内で動作するアプリケーションにて使用されたファイルのクローズ要求が発生されたときに、当該ファイルのデータを用いて所定の規則に従って第一の署名情報を作成する第一の署名情報作成手段と、該第一の署名情報をクローズ要求に係るファイルと関連付けて記憶装置内に格納する署名情報格納制御手段とを備えるように構成される。

【0009】

このようなファイファイル処理ユニットでは、特に、署名情報の作成に関する専用アプリケーションを立ち上げることなく、所望のアプリケーションにて使用されたファイルのクローズ要求が発生されると、そのファイルのデータを用いて第一の署名情報が作成されると共に、その第一の署名情報がオープン要求に係るファイルと関連付けられて記憶装置に格納される。従って、所望のアプリケーションでのファイルクローズ処理に際して、簡単に署名情報の作成ができるようになる。

【0010】

上記ファイル処理ユニットにおいて、上記第一の署名情報は、請求項2に記載されるように、クローズ要求に従って当該ファイルが記憶装置に格納された後に、該ファイルのデータを記憶装置から読み出すクローズファイル読み出し手段を有し、該クローズファイル読み出し手段にて読み出されたデータを用いて第一の署名情報を作成するように構成することができる。

【0011】

また、上記各ファイル処理ユニットにおいて、上記署名情報格納制御手段は、請求項3に記載されるように、クローズ要求に係るファイルに第一の署名情報を付加する署名情報付加手段を有し、当該クローズ要求に係るファイルと第一の署名情報を一体的に記憶装置に格納するように構成することができる。

特定のファイルにのみ署名情報を付加することができるという観点から、本発

明は、請求項4に記載されるように、上記各ファイル処理システムにおいて、上記クローズ要求時にクローズ要求に係るファイルに署名情報を付加すべきか否かを判定する署名付加判定手段を有し、当該クローズ要求に係るファイルに署名情報を付加すべきであると署名付加判定手段が判定したときに、上記第一の署名情報作成手段が第一の署名情報を作成するように構成することができる。

#### 【0012】

このようなファイル処理ユニットでは、種々の属性を有するファイルを扱うコンピュータシステムにおいて、クローズ要求がアプリケーションから発せられたときに、署名情報を付加すべきファイルについてのみ署名情報が付加されるようになる。

アプリケーションにてファイルを使用する前に、ファイルに署名情報を付加するか否かを決定できるという観点から、本発明は、請求項5に記載されるように、上記ファイル処理ユニットにおいて、アプリケーションにてファイルが使用される前に、少なくともクローズ要求に係るファイルに署名情報を付加する処理モードの設定を行うモード設定手段を有し、上記署名付加判定手段は、予め設定された処理モードに基づいて当該クローズ要求に係るファイルに署名情報を付加すべきか否かを判定するモード判定手段を有するように構成することができる。

#### 【0013】

アプリケーションからのファイルのオープン要求が発せられたときに、そのオープン要求に係るファイルに関連付けられて記憶装置に格納された第一の署名情報のチェックを行えるという観点から、本発明は、請求項6に記載されるように、上記各ファイル処理ユニットにおいて、上記アプリケーションで使用すべきファイルのオープン要求が発せられたときに、そのオープン要求に応答して、当該ファイルのデータを用いて上記所定の規則に従って第二の署名情報を作成する第二の署名情報作成手段と、オープン要求に係るファイルに関連付けられて上記記憶装置内に格納された第一の署名情報と上記第二の署名情報とが一致するか否かを判定する署名一致判定手段と、アプリケーションに提供すべき上記署名一致判定手段での判定結果を表す情報を作成する判定結果作成手段とを有するように構成することができる。

## 【0014】

上記ファイル処理ユニットにおいて、上記第二の署名情報作成手段は、請求項6に記載されるように、オープン要求に係る処理が完了する前に、オープン要求に係るファイルのデータを記憶装置から読み出すオープンファイル読み出し手段を有し、該オープンファイル読み出し手段にて読み出されたデータを用いて第二の署名情報を作成するように構成することができる。

## 【0015】

また、特定のファイルについてのみ署名情報のチェックを行うことができるという観点から、本発明は、請求項8に記載されるように、上記ファイル処理システムにおいて、上記オープン要求時にオープン要求に係るファイルに対応付けられて記憶装置内に格納された第一の署名情報のチェックを行うべきか否かを判定する署名チェック判定手段を有し、当該オープン要求に係るファイルに対応付けられて記憶装置内に格納された第一の署名情報のチェックを行うべきであると署名チェック判定手段が判定したときに、上記第二の署名情報作成手段が上記第一の署名情報との一致を判定すべき第二の署名情報を作成するように構成することができる。

## 【0016】

また、アプリケーションにてファイルを使用する前に、ファイルに関連付けて記憶装置に格納された署名情報をチェックすべきか否かを決定できるという観点から、本発明は、請求項9に記載されるように、上記ファイル処理システムにおいて、上記署名チェック判定手段は、アプリケーションにてファイルが使用される前に、少なくともオープン要求に係るファイルに関連付けて記憶装置に格納された第一の署名情報のチェックを行う処理モードの設定を行うモード設定手段を有し、上記署名チェック判定手段は、予め設定された処理モードに基づいて当該オープン要求に係るファイルに関連づけて記憶層内に格納された第一の署名情報のチェックを行うべきか否かを判定するモード判定手段を有するように構成することができる。

## 【0017】

更に、上記本発明の課題を解決するため、本発明は、請求項10に記載される

ように、コンピュータシステム内で動作するアプリケーションにて使用すべきファイルのオープン要求が発せられたときに、そのオープン要求に応答して、当該ファイルのデータを用いて所定の規則に従って第二の署名情報を作成する第二の署名情報作成手段と、オープン要求に係るファイルのデータを用いて予め上記所定の規則に従って作成され、該ファイルに関連付けられて記憶装置内に格納された第一の署名情報と上記第二の署名情報とが一致するか否かを判定する署名一致判定手段と、アプリケーションに提供すべき上記署名一致判定手段での判定結果を表す情報を作成する判定結果作成手段とを有するように構成される。

## 【0018】

このようなファイル処理ユニットでは、ファイルに関連付けられて記憶装置に格納された署名情報をチェックするための専用のアプリケーションを立ち上げることなく、所望のアプリケーションからオープン要求が発せられたときに、その要求に係るファイルに関連付けられて記憶装置に格納された第一の署名情報と、その要求に係るファイルのデータを用いて作成された第二の署名情報とが一致するか否かが判定される。そして、その判定結果が作成される。従って、所望のアプリケーションでのファイルオープン処理に際して、簡単に署名情報のチェックができるようになる。

## 【0019】

上記第二の署名情報作成手段は、請求項10に記載されるように、オープン要求に係る処理が完了する前に、オープン要求に係るファイルのデータを記憶装置から読み出すオープンファイル読み出し手段を有し、該オープンファイル読み出し手段にて読み出されたデータを用いて第二の署名情報を作成するように構成することができる。

## 【0020】

更に、上記本発明の課題を解決するため、本発明は、請求項14に記載されるように、アプリケーションからのイベントに基づいてファイルに対する処理を実行するファイルシステムを有するコンピュータシステムに適用されるファイル処理ユニットにおいて、アプリケーションからのファイルクローズのイベントに係るファイルに対するファイルシステムでの処理が完了する前に、該ファイルクロー

ズのイベントを受け取りそのイベントに係るファイルのデータを用いて所定の規則に従って第一の署名情報を作成する第一の署名情報作成手段と、該第一の署名情報を上記ファイルクローズのイベントに係るファイルに関連付けて記憶装置に格納する署名情報格納制御手段と、上記第一の署名情報が作成された後に、上記ファイルクローズのイベントに係るファイルに対する上記ファイルシステムでの処理への復帰処理を行う第一の復帰手段とを備えるように構成することができる。

【0021】

このようなファイル処理ユニットでは、コンピュータシステム内のファイルシステムがアプリケーションからのクローズイベントに基づいて処理を行う際に、当該ファイル処理ユニットがクローズイベントを受け取って、そのイベントに係るファイルのデータを用いて第一の署名情報を作成する。そして、その第一の署名情報が当該ファイルと関連付けられて記憶装置に格納される。この第一の署名が作成された後、ファイル処理ユニットは、クローズイベントに係るファイルに対する上記ファイルシステムへの復帰処理を行う。

【0022】

このため、ファイルシステム及びアプリケーションがファイルクローズに係る処理を実行している間に、自動的に第一の署名情報が作成され、その第一の署名情報が当該ファイルに関連付けられて記憶装置に格納される。

また、更に、上記本発明の課題を解決するため、本発明は、請求項15に記載されるように、アプリケーションからのイベントに基づいてファイルに対する処理を実行するファイルシステムを有するコンピュータシステムに適用されるファイル処理ユニットにおいて、アプリケーションからのファイルクローズのイベントに係るファイルに対するファイルシステムでの処理が完了する前に、該ファイルクローズのイベントを受け取りそのイベントに係るファイルのデータを用いて所定の規則に従って第二の署名情報を作成する第二の署名情報作成手段と、オープン要求に係るファイルのデータを用いて予め上記所定の規則に従って作成され、該ファイルに関連付けられて記憶装置内に格納された第一の署名情報と上記第二の署名情報とが一致するか否かを判定する署名一致判定手段と、アプリケーション



ョンに提供すべき上記署名一致判定手段での判定結果を表す情報を作成する判定結果作成手段と、上記判定結果を表す情報が作成された後に、上記判定結果を表す情報をファイルシステムに渡すと共に、上記ファイルオープンのイベントに係るファイルに対する上記ファイルシステムでの処理への復帰処理を行う第二の復帰手段とを備えるように構成される。

【0023】

上記のようなファイル処理ユニットでは、コンピュータシステム内のファイルシステムがアプリケーションからのオープンイベントに基づいて処理を行う際に、当該ファイル処理ユニットがオープンイベントを受け取って、そのイベントに係るファイルのデータを用いて第二の署名情報を作成する。そして、当該ファイルに関連付けられて記憶装置に格納された第一の署名情報と上記第二の署名情報とが一致するか否かが判定される。そして、当該ファイル処理ユニットは、その判定結果をファイルシステムに提供すると共に、オープンイベントに係るファイルに対する上記ファイルシステムへの復帰処理を行う。

【0024】

このため、ファイルシステム及びアプリケーションがファイルクオープンに係る処理を実行している間に、自動的に第二の署名情報が作成され、その予めファイルに対応するものとして作成された第一の署名情報と当該第二の署名情報とが一致する否かがチェックされる。

上記ファイル処理ユニットの機能をコンピュータシステムに容易に適用させることができるという観点から、本発明は、請求項16に記載されるように、上記ファイル処理ユニットが当該コンピュータシステムに接続される外部ユニットとして構成されるようにできる。

【0025】

また、上記外部ユニットは、請求項17に記載されるように、PCカードとすることができる。

【0026】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。

本発明の実施の一形態に係るファイル処理ユニットが適用されるコンピュータシステムのハードウェア構成は、例えば、図1に示すようになっている。

図1において、このシステムは、CPU10、メモリユニット12、入力ユニット14、表示ユニット16、ハードディスクドライブユニット（HDD）18及びインターフェース回路22を有している。上記各ユニット及びインターフェース回路22は、それぞれバスに接続されている。

#### 【0027】

メモリユニット12には、オペレーションシステム（OS）や種々のアプリケーションが格納され、CPU10は、メモリユニット12内のOSに従った処理及び選択されたアプリケーションを実行する。入力ユニット14は、マウス及びキーボードを有し、アプリケーションの選択、選択されたアプリケーションによってオープンされたファイルに対するデータの入力、必要なモード設定、その他必要な情報を入力するために使用される。

#### 【0028】

表示ユニット16は、各種制御画面、アプリケーションによってオープンされたファイルの情報等を表示する。ハードディスクドライブユニット18は、ハードディスク20を駆動し、選択されたアプリケーションやOSに基づいたCPU10からの指令に従ってハードディスク20へのファイルの格納、読み出しを行う。

#### 【0029】

インターフェース回路22にはPCカード100が接続される。PCカード100は本発明に係るファイル処理ユニットとしてのドライバを有し、インターフェース回路22は、CPU10にて実行されるアプリケーションや例えばOS内に構築されるファイルシステムとPCカード100内のドライバとの間のインタフェースを行う。

#### 【0030】

上記のようなコンピュータシステムを立ち上げた状態で、PCカード100をインターフェース回路22にセットすると、OS内に構築されるファイルシステムとPCカード100内のドライバとの間で、例えば、図2に示す手順に従って初

期処理が実行される。図2において、ファイルシステムがドライバ確認コマンドをドライバに対して送ると（S1）、ドライバは、初期処理の開始可能な状態にあるか否かを判定する（S2）。この判定の結果、ドライバが初期処理の開始可能な状態にない場合には、ドライバはエラー応答（NG応答）をファイルシステムに返送する。このエラー応答を受信したファイルシステムは、システムにセットされたドライバが起動できる状態ではないとして、所定のエラー処理を実行する（S3）。このエラー処理では、例えば、セットされたドライバが起動しない旨のメッセージを出力する。このメッセージは、表示ユニット16に表示される。

#### 【0031】

一方、ドライバが上記初期処理の開始可能な状態なある場合には、ドライバは正常応答（OK応答）をファイルシステムに返送する。この正常応答を受信したファイルシステムは、当該ドライバを特定する情報をメモリユニット14に登録する（S4）。そして、ファイルシステムは、例えば、セットされたドライバが登録された旨のメッセージを出力する。このメッセージは、表示ユニット16に表示される。

#### 【0032】

上記のようにしてPCカード100をインタフェース回路22に接続し、PCカード100内のドライバがファイルシステムに登録されると、引き続き、図3に示す手順に従って処理が実行される。図3において、ドライバの登録を確認したファイルシステムは、初期処理の実行をドライバに対して指示する（S11）。この指示を受信したドライバは、動作を開始し（S12）、アプリケーションからファイルシステムに送られるイベントをドライバに渡す（フックする）要求をファイルシステムに対して送る（S13）。

#### 【0033】

この要求を受信したファイルシステムは、その要求が許容できる場合には、イベントをドライバに渡す際に指定すべきアドレス（フックアドレス）を登録すると共に、許容応答をドライバに返す（S14）。一方、ドライバでの処理が不完全の場合や、ファイルシステムがドライバからの要求の受信に失敗した場合等に

は、ファイルシステムはドライバに対して要求エラーの応答を返す（S14）。

【0034】

上記のような応答を受信したドライバは、返送された応答が許容応答かエラー応答であるかの判定を行う（S15）。その応答が許容応答であれば、初期処理は正常に終了する。一方、その受信した応答がエラー応答であれば、要求が失敗したとして、初期処理の再試行あるいは所定のエラー処理が実行される。

上記のようにしてドライバの登録及び初期処理が終了した状態で、ユーザが入力ユニット14を用いて必要なアプリケーションの指定を行うと、指定されたアプリケーションがハードディスク20からハードディスクドライブユニット18を介してメモリユニット12に転送される。そして、そのアプリケーションの起動を行うと、例えば、図4に示す手順に従って、ユーザ認証及びモード設定の処理が実行される。

【0035】

起動されたアプリケーションは、ユーザID及びパスワードの入力画面を表示ユニット16に表示させる。そして、図4において、ユーザが入力ユニット14を用いてユーザID及びパスワードを入力すると、アプリケーションは、そのユーザID及びパスワードを取得し（S21）、入力されたユーザID及びパスワードのチェックを行う（S22）。このチェックの結果、ユーザ認証がなされなかった場合には、所定のエラー処理が行われる。

【0036】

一方、上記ユーザID及びパスワードによってユーザ認証がなされた場合には、アプリケーションはユーザが入力ユニット14を用いて指定したフォルダ及び設定した処理モード（モード値）をOSを介してドライバに送る（S23）。この処理モードは、図9に示すように、ファイルオープンときに著名のチェックを行うか否か、ファイルクローズのときに署名作成を行うか否か、ライト処理のときにデータの暗号化・圧縮を行うか否か、リード処理のときにデータの復号・伸長を行うか否かに基づいて16通りの処理モードが予め定められている。この図9に示す各モード値と処理内容との関係は、モードテーブルとしてドライバ内のメモリに予め格納されている。

【0037】

また、上記のように処理モードの設定と共にフォルダが指定されると、処理モードとフォルダとが対応付けられ、例えば、図10に示すようなテーブルとしてドライバのメモリ内に保存される。このようにフォルダと処理モードとの関係が定められることにより、各処理モードにて処理されるべきファイルは、その処理モードに対応したフォルダに格納されることになる。

【0038】

上記処理モードの設定及びフォルダの指定が終了すると、アプリケーションは動作開始の指示をOSを介してドライバに送る(S25)。そして、その指示を受信したドライバは、アプリケーションから発行されるイベント(ファイルオープン、ファイルクローズ、リード、ライト)に基づいた設定された処理モードでの動作を開始する。

【0039】

以下、モード値15(図9参照)が設定されると共に、フォルダP(図10参照)が指定された場合を例に説明する。

上記のような処理によりアプリケーション及びドライバが有効となっている状態で、ユーザがあるファイルのデータについて処理するために、ファイルオープンに係る操作を行うと、例えば、図5に示す手順に従って処理が実行される。

【0040】

ユーザの操作に基づいてアプリケーションからオープン関数が発行される(S31)。このオープン関数は、ファイルシステム(OS)に渡される。すると、ファイルシステムは、上記のようにした登録されたドライバ(図2参照)に対してフックアドレスと共にオープンイベントを渡し(S32)、ファイルのオープン処理を開始する(S33)。オープンイベントには、

- 指定されたフォルダ名、
- ファイル名(パス名を含む)、
- ファイル属性、
- オープン関数のパラメータ、
- ファイルシステムへの復帰アドレス等

が含まれる。

【0041】

ドライバは、ファイルシステムからオープンイベントを受信すると（S34）、以下の手順で処理を実行する。

まず、指定されたフォルダのチェックが行われる（S35）。この処理では、図10に示すテーブルを参照して、ドライバにて処理（暗号化、復号、署名作成、署名チェック）を行うべきファイルが格納されたフォルダとして登録されているか否かが判定される。この例の場合、指定されたフォルダPが処理対象のフォルダとして登録されているので（図10参照）、更に、ドライバは指定されたファイルの属性を属性テーブル（図示せず）を参照してチェックする（S36）。これは、指定されたファイルが、著名の付加や暗号化を行ってもよいファイルか否かをチェックするために行われる。システムファイル、隠しファイル、ドライバファイル等については、署名の付加や暗号化が行えないことを示す属性値が予め登録されている。

【0042】

指定されたファイルが上記のような署名の付加や暗号化の対象となっていないファイルの場合、属性テーブルの当該指定ファイルに対して、処理中であることを示すファイルハンドルが保存される（S37）。そして、モードテーブルを参照して、設定された処理モードがオープン時に処理を行うべきモードであるか否かが判定される（S38）。この例の場合、モード値15が設定されているので、ファイルオープン時に署名チェックを行うべき処理モードであると判定される。

【0043】

すると、ドライバは指定されたファイルのリード要求をハードディスクドライブユニット18に出力する（S39）。この要求に対して、ハードディスクドライブ（HDD）ユニット18は、ハードディスク20から指定されたファイルのデータを読み出し、そのデータをドライバに返す（S40）。

ハードディスクドライブユニット18からデータを受信すると、ドライバは、受信したデータの全部または一部を用いて所定の規則に従って署名データ（A）

を作成（S41）。そして、更に、後述するように（ファイルクローズ時の処理）この指定されたファイルのデータ領域と別の領域に既に添付された署名データ（B）のリード要求をハードディスクドライブユニット18に出力する（S42）。この要求に対して、ハードディスクドライブユニット18は、ハードディスク20から指定されたファイルの所定領域から署名データ（B）を読み出し、その署名データ（B）をドライバに返す（S43）。

#### 【0044】

ハードディスクドライブユニット18からデータを受信すると、ドライバは、受信した署名データ（B）と上記のように作成した署名データ（A）とを比較し、それらが一致するか否かを判定する（S44）。これらの署名データ（A）及び（B）が一致すると、正常ステータスが設定される（S45）。そして、ドライバは、正常ステータスをファイルシステムに渡すと共に、ファイルシステムの復帰アドレスへの復帰処理を実行する（S47）。

#### 【0045】

ファイルシステムは、復帰アドレスへの復帰を受けて、その復帰アドレスからのオープン処理を継続し、ドライバからの正常ステータスを確認した後にオープン処理を完了する（S48）。そして、そのオープン処理の結果（オープンすべきファイルのデータ等）をアプリケーションに渡す。

このオープン処理の結果を受けたアプリケーションは、オープン関数に復帰する（S49）。その結果、アプリケーションにおいてユーザに指定されたファイルがオープンされる。

#### 【0046】

一方、指定されたファイルに既に添付された署名データ（B）と新たに作成された署名データ（A）とが不一致の場合（S44でNG）、ドライバは、オープンエラーを設定し（S46）、ファイルシステムの復帰アドレスへの復帰処理に際してそのオープンエラーのステータスをファイルシステムに渡す。この場合、ファイルシステムは、このオープンエラーを確認してオープン処理の完了を完了する（S48）。そして、オープン処理の結果と共にオープンエラーのステータスがファイルシステムからアプリケーションに渡される。その結果、アプリケー

ションにおけるオープン関数への復帰によって、ファイルがオープンされると共に、ファイルのデータが改ざんされた可能性のある旨の表示等が行われる。

【0047】

なお、上記オープンイベントに基づいた処理の過程で、指定されたフォルダがオープン時に署名チェックを行う処理モードに対応するものとして設定されていない場合（S35でNG）や、指定されたファイルが署名を必要としない属性を有するものである場合（S36でNG）、ドライバは、上述したような署名のチェックを行わずに、そのままファイルシステムの復帰アドレスへの復帰処理を実行する（S47）。

【0048】

上記のように、ユーザによるオープン操作に基づいてアプリケーションからオープン関数がファイルシステムに発行されると、ドライバにて署名のチェックが自動的に実行され、そのチェック結果がファイルシステムに返される。そして、ファイルシステムは、通常のオープン処理を実行し、そのオープン処理の結果と署名のチェック結果をアプリケーションに返す。従って、ユーザは、特に署名チェックのための専用のアプリケーションを立ち上げることなく、所望のアプリケーションを立ち上げた状態で、ファイルオープンの際に、処理モードの設定をするだけで、オープン処理の対象となるファイルの署名チェックの結果を得ることができる。

【0049】

上記のようにしてオープンされたファイルに対するリード処理は、例えば、図6に示すような手順に従って実行される。

図6において、アプリケーションからリード関数がファイルシステムに対して発行される（S51）。このリード関数を受けたファイルシステムは、リードイベントをドライバに渡すと共に（S52）、リード処理を開始する（S53）。そして、このリードイベントを受信した（S54）ドライバは、以下のような処理を実行する。

【0050】

なお、リードイベントは、



ファイル名（パス名を含む）

ファイルハンドル

リードポイント

リードバッファ

リードサイズ

ファイルシステムへの復帰アドレス等

を含む。

#### 【0051】

ファイルオープンの場合と同様にフォルダのチェックを行った後に（S55）、ファイル属性のチェックが行われる（S56）。このフォルダのチェックでは、図9及び図10に示すテーブルを参照して、指定されたフォルダがリード時にデータの復号・伸長を行うファイルを格納した復号・伸長処理の対象となるフォルダであるか否かが判定される。また、ファイル属性のチェックでは、指定されたファイルに対して属性テーブルに要求に係るファイルハンドルが設定されているか否かが判定される。これは、指定されたファイルがリード時の処理対象となるファイルであるか否かを判定するためのものである。この例場合、フォルダPがモード値15に対応するものとして設定されているので、リード時にデータの復号・伸長を行うファイルが格納されたフォルダであると判定される。そして、指定されたファイルが、ファイルオープン時に前述したようにファイルハンドルがファイル属性として設定されているファイルであるので、要求に係るハンドルが設定されていると判定される。

#### 【0052】

上記の各チェックの後、更に、モードチェックが行われる（S57）。このモードチェックでは、モードテーブルを参照して、設定された処理モードがリード時にデータの復号・伸長を行うモードであるか否かが判定される。この場合、モード値15が設定されているので、リード時にデータの復号・伸長を行うモードとして判定される。

#### 【0053】

その後、指定されたファイルのデータの読み出し要求がドライバからハードデ

ィスクドライブユニット18に出力される(S58)。この要求を受けたハードディスクドライブユニット18は、ハードディスク20からバウンダリを考慮して指定されたファイルのデータを読み出し、そのデータをドライバに渡す(S59)。この読み出されたデータは、後述するように所定のアルゴリズムに従って既に暗号化・圧縮されている。

#### 【0054】

ドライバは、このデータをハードディスクドライブユニット18から受信すると、そのデータについて復号処理を行う(S60)。この復号処理では、例えば、8バイト単位で上記暗号化・圧縮のアルゴリズムに対応するアルゴリズムに従ってデータの復号・伸長及び、端数処理を実行する。また、この復号処理では、読み出したデータの8バイトが復号・伸長されたデータの8バイトに対応するようにしている。その結果、データ長から両者の区別がつかないようになっている。

#### 【0055】

上記の復号処理が終了すると、リードサイズ分のデータがリードバッファに設定され(S61)、ファイルシステムの復帰アドレスへの復帰処理が実行される(S62)。ファイルシステムは、復帰アドレスへの復帰を受けて、その復帰アドレスからのリード処理を継続し、ドライバのリードバッファに設定されたデータを取得すると共にリード処理を完了する(S63)。そして、そのリード処理の結果(リードデータ)をアプリケーションに渡す。

#### 【0056】

このリード処理の結果を受けたアプリケーションは、リード関数に復帰する(S64)。その結果、アプリケーションがリードデータを取得し、そのアプリケーションでの処理により、例えば、リードデータが表示ユニット16に表示される。

なお、上記リードイベントに基づいた処理の過程で、指定されたフォルダがリード時に復号・伸長を行う処理モードに対応するものとして設定されていない場合(S55でNG)や、指定されたファイルに対して要求されたファイルハンドが設定されていない場合(S56でNG)、また、設定された処理モードがリー

ド時に復号・伸長を行う処理モードではない場合（S57でNO）、ドライバは、上述したような復号処理を行わずに、そのままファイルシステムの復帰アドレスへの復帰処理を実行する（S47）。その結果、ファイルシステムでのリード処理により、通常と同様に、リードデータがファイルシステムからアプリケーションに渡される。

【0057】

上記のように、ファイルのリード時において、アプリケーションからリード関数が発行されると、ドライバにて、リード処理の対象となるファイルのデータの復号・伸長処理が自動的に実行され、その復号・伸長されたデータがファイルシステムに返される。そして、ファイルシステムは、通常のリード処理を実行し、そのリード処理の結果として復号・伸長されたデータをアプリケーションに返す。従って、ユーザは、暗号化・圧縮されたデータについて特に復号・伸長の処理について意識することなく、所望のアプリケーションを立ち上げた状態で、暗号化・圧縮されたデータを元のデータに復号・伸長した状態で得ることができる。

【0058】

また、上記のようにしてオープンされたファイルに対するライト処理は、例えば、図7に示すような手順に従って実行される。

図7において、アプリケーションからライト関数がファイルシステムに対して発行される（S71）。このライト関数を受けたファイルシステムは、ライトイベントをドライバに渡すと共に（S72）、ライト処理を開始する（S73）。そして、このライトイベントを受信した（S74）ドライバは、以下のような処理を実行する。

【0059】

なお、ライトイベントは、  
ファイル名（パス名を含む）  
ファイルハンドル  
ライトポイント  
ライトデータ  
ライトバッファ

ライトサイズ

ファイルシステムへの復帰アドレス等  
を含む。

【0060】

ファイルオープン及びリード処理の場合と同様にフォルダのチェックを行った後に（S75）、ファイル属性のチェックが行われる（S76）。このフォルダのチェックでは、図9及び図10に示すテーブルを参照して、指定されたフォルダがライト時にデータの暗号化・圧縮を行うファイルを格納した暗号化・圧縮処理の対象となるフォルダであるか否かが判定される。また、ファイル属性のチェックでは、指定されたファイルに対して属性テーブルに要求に係るファイルハンドルが設定されているか否かが判定される。この例場合、フォルダPがモード値15に対応するものとして設定されているので、ライト時にデータの暗号化・圧縮を行うファイルが格納されたフォルダであると判定される。そして、指定されたファイルが、ファイルオープン時に前述したようにファイルハンドルがファイル属性として設定されているファイルであるので、要求に係るハンドルが設定されていると判定される。

【0061】

上記の各チェックの後、更に、モードチェックが行われる（S77）。このモードチェックでは、モードテーブルを参照して、設定された処理モードがライト時にデータの暗号化・圧縮を行うモードであるか否かが判定される。この場合、モード値15が設定されているので、ライト時にデータの暗号化・圧縮を行うモードとして判定される。

【0062】

その後、指定されたファイルのデータの読み出し要求がドライバからハードディスクドライブユニット18に出力される（S78）。この要求を受けたハードディスクドライブユニット18は、ハードディスク20からバウンダリを考慮して指定されたファイルのデータを読み出し、そのデータをドライバに渡す（S79）。この読み出されたデータは、後述するように所定のアルゴリズムに従って既に暗号化・圧縮されている。

## 【0063】

ドライバは、このデータをハードディスクドライブユニット18から受信すると、そのデータについて復号処理を行う（S80）。この復号処理では、前述したリード時の処理と同様に暗号化・圧縮のアルゴリズムに対応したアルゴリズムに従って、8バイト単位でデータの復号・伸長及び、端数処理がなされる。

上記の復号処理が終了すると、上記のように読み出されて復号処理によって元のデータの戻されたデータにライトデータが上書きされる（S81）。そして、この読み出されたデータに上書きされたライトデータの暗号化処理が実行される（S82）。この暗号化処理では、所定のアルゴリズムに従って8バイト単位でデータの暗号化・圧縮及び、端数処理がなされる。このとき、暗号化前のデータ8ビットが暗号化されたデータ8ビットに対応するようにデータの暗号化・圧縮がなれ、データ長から両者の区別がつかないようにしている。

## 【0064】

このような暗号化処理が終了すると、ドライバはハードディスクドライブユニット18にライト処理を要求する（S83）。この要求に応答してハードディスクドライブユニット18は、上記暗号化・圧縮されたデータをバウンダリーを考慮してハードディスク20の指定されたファイルに書き戻し、その応答をドライバに返す（S83）。

## 【0065】

暗号化・圧縮されたデータの書き込み（ライト）が終了した後に、ドライバは、ファイルシステムへの復帰処理を実行する（S86）。ファイルシステムは、ライト処理の完了した状態（S85）で復帰アドレスへの復帰を受けて、ライト処理の結果をアプリケーションに渡す。

このライト処理の結果を受けたアプリケーションは、ライト関数に復帰する（S87）。

## 【0066】

なお、上記ライトイベントに基づいた処理の過程で、指定されたフォルダがライト時に暗号化・圧縮を行う処理モードに対応するものとして設定されていない場合（S75でNG）や、指定されたファイルに対して要求されたファイルハン

ドが設定されていない場合（S 7 6でNG）、また、設定された処理モードがライト時に暗号化・圧縮を行う処理モードではない場合（S 7 7でNO）、ドライバは、上述したような暗号化処理を行わずに、そのままファイルシステムの復帰アドレスへの復帰処理を実行する（S 4 7）。その結果、ファイルシステムでのライト処理により、通常と同様に、アプリケーションからのライトデータがファイルシステムからハードディスクドライブユニット 1 8 に渡され、そのライトデータがハードディスク 2 0 の指定されたファイルに書き込まれる。

## 【0067】

上記のように、ファイルのライト時において、アプリケーションからライト関数が発行されると、ドライバにて、ライトデータの暗号化・圧縮処理が自動的に実行され、その暗号化・圧縮されたデータが指定されたファイルに書き込まれる。そして、ファイルシステムは、通常のライト処理と同様にその処理結果をアプリケーションに戻す。従って、ユーザは、暗号化・圧縮について特に意識することなく、所望のアプリケーションを立ち上げた状態で、暗号化・圧縮されたデータがファイルに格納される。

## 【0068】

上述したようにオープンされたファイルに対するクローズ処理は、例えば、図 8 に示す手順に従って実行される。

図 8 において、ユーザの操作に基づいてアプリケーションからクローズ関数が発行される（S 3 1）。このクローズ関数は、ファイルシステムに渡される。すると、ファイルシステムは、ドライバに対してドライバにオープンイベントを渡し（S 9 2）、ファイルのクローズ処理を開始する（S 9 3）。クローズイベントには、

ファイル名（パス名を含む）、

ファイル属性、

ファイルシステムへの復帰アドレス等

が含まれる。

## 【0069】

ドライバは、ファイルシステムからクローズイベントを受信すると（S 9 4）

、以下の手順で処理を実行する。

まず、ファイルオープン時の処理と同様に、フォルダのチェックを行った後に（S95）、ファイル属性のチェックが行われる（S96）。このフォルダのチェックでは、図9及び図10に示すテーブルを参照して、指定されたフォルダがクローズ時に署名データの作成を行うファイルを格納した署名作成処理の対象となるフォルダであるか否かが判定される。また、ファイル属性のチェックでは、指定されたファイルに対して属性テーブルに要求に係るファイルハンドルが設定されているか否かが判定される。この例場合、フォルダPがモード値15に対応するものとして設定されているので、クローズ時に署名データの作成を行うファイルが格納されたフォルダであると判定される。そして、指定されたファイルが、ファイルオープン時に前述したようにファイルハンドルがファイル属性として設定されているファイルであるので、要求に係るハンドルが設定されていると判定される。

#### 【0070】

上記の各チェックの後、更に、モードチェックが行われる（S97）。このモードチェックでは、モードテーブルを参照して、設定された処理モードがファイルクローズ時に署名データを作成するモードであるか否かが判定される。この場合、モード値15が設定されているので、設定された処理モードがファイルクローズ時に署名データを作成するモードであると判定される。

#### 【0071】

次いで、ドライバは指定されたファイルのリード要求をハードディスクドライブユニット18に出力する（S98）。この要求に対して、ハードディスクドライブ（HDD）ユニット18は、ハードディスク20から指定されたファイルのデータを読み出し、そのデータをドライバに返す（S99）。

ハードディスクドライブユニット18からデータを受信すると、ドライバは、受信したデータの全部または一部を用いて所定の規則に従って署名データ（B）を作成する（S100）。そして、この作成され署名データ（B）を指定されたファイルに付加する要求がドライバからハードディスクドライブユニット18になされる（S101）。すると、ハードディスクドライブユニット18は、指定

されたファイルのデータ領域と別の所定領域に作成された署名データ（B）を格納する（S102）。

【0072】

ドライバは、上記のように署名データ（B）を指定ファイルに付加する要求をハードディスクドライブユニット18行った後に、属性テーブルにおける指定ファイルに対応したファイルハンドルを消去する（S103）。その後、正常ステータスが設定される（S104）。そして、ドライバは、正常ステータスをファイルシステムに渡すと共に、ファイルシステムの復帰アドレスへの復帰処理を実行する（S105）。

【0073】

ファイルシステムは、復帰アドレスへの復帰を受けて、その復帰アドレスからのクローズ処理を継続し、ドライバからの正常ステータスを確認した後にクローズ処理を完了する（S106）。そして、そのクローズ処理の結果をアプリケーションに渡す。

このクローズ処理の結果を受けたアプリケーションは、クローズ関数に復帰する（S107）。その結果、アプリケーションにおいてユーザに指定されたファイルがクローズされる。

【0074】

なお、上記クローズイベントに基づいた処理の過程で、指定されたフォルダがクローズ時に署名データの作成を行う処理モードに対応するものとして設定されていない場合（S95でNG）や、指定されたファイルがについてファイルハンドルが設定されていない場合（S96でNG）、ドライバは、上述したような署名データ（B）の作成を行わずに、そのままファイルシステムの復帰アドレスへの復帰処理を実行する（S105）。

【0075】

また、上記モードチェックの結果、設定された処理モードがファイルオープン時に署名データを作成するモードでない場合は（モード値0～3、8～11）、正常ステータスが設定された後に（S104）、ファイルシステムの復帰アドレスへの復帰処理が実行される（S105）。



上記のように、ユーザのクローズ操作に基づいてアプリケーションからクローズ関数がファイルシステムに発行されると、ドライバにて署名データ（B）が自動的に作成され、その署名データ（B）がクローズ処理に係るファイルに付加された状態で当該ファイルがクローズされる。従って、ユーザは、特に署名の作成を意識することなく、所望のアプリケーションを立ち上げた状態で、ファイルクローズを行うだけで、署名データが添付された状態で当該ファイルがクローズされる。

## 【0076】

上述した例では、オープンイベント発行の際に署名データのチェック、リードイベント発行の際に暗号化・圧縮されたファイルデータの復号・伸長、ライトイベント発行の際に暗号化・圧縮、クローズイベント発行の際に署名データの作成を行う処理モード（モード値15：図10参照）が設定されたが、他のモードが設定された場合であっても、当該設定された処理モードにて有効となるオープンイベント発行の際の処理、リードイベント発行の際の処理、ライトイベント発行の際の処理及びクローズイベント発行の際の処理のうちの1または複数の処理が行われる。

## 【0077】

例えば、暗号化・圧縮化されたファイルデータがCD-ROM等の媒体から提供される場合等では、モード値1を設定することができる。この場合、ファイルオープンをした後に、リードイベントが発行されたときに、当該暗号化・圧縮されたファイルデータが自動的に復号・伸長され、ユーザが当該ファイルデータの利用を行うことができる。例えば、作成したファイルデータを暗号化・圧縮してフロッピーディスク等の媒体に格納し、該媒体を他のシステムに供給する場合等では、モード値2を設定することができる。この場合、ファイルオープンした後、ライトイベントが発行されたときに、当該ファイルのデータが自動的に暗号化・圧縮された状態でフロッピーディスク等の媒体に格納される。

## 【0078】

また、例えば、ファイルに署名データを添付した状態でフロッピーディスク等の媒体に格納し、該媒体を他のシステムに供給する場合等では、モード値3を設

定することができる。この場合、ファイルオープンした後、リード、ライトのイベントに基づいた処理が実行され、更に、ファイルクローズのイベントが発行されたときに、当該クローズされるファイルに対して自動的に署名データが添付される。更に、例えば、署名データが添付されたファイルがCD-ROM等の媒体にて提供される場合等では、モード値4を設定することができる。この場合、ファイルのオープンイベントが発行されたときに、自動的に、当該ファイルのデータに基づいて署名データが作成され、その作成された署名データとファイルに添付された署名データが一致するか否かが判定される。そして、各署名データが一致する場合のみ、そのファイルのデータの利用が可能となる。

## 【0079】

また、上述した例では、署名データがクローズ要求に係るファイルのデータ領域と異なる領域に追加されるようにしたが、署名データを他のファイルに格納し、その署名データのファイルを上記データのファイルに関連づけハードディスク20等の記憶装置に格納することもできる。

更に、上記例では、ファイルを格納する記憶装置は、ハードディスク20であったが、通常のコンピュータシステムの記憶装置として使用できるものであれば特に限定されない。また、署名データのチェック及び暗号化・圧縮データの復号・伸長の少なくともいずれか一方を行う処理モード（モード値1、8または9）では、読み取り専用の記憶媒体（CD-ROM等）を記憶装置として用いることができる。

## 【0080】

上記例では、本発明のファイル処理ユニットの実施の形態となるドライバは、PCカード内に構成されたが、ICカードや他の外部装置内に構成することも可能である。更に、当該ドライバは、コンピュータシステム内で実行される他のプログラムとして実現することも可能である。

上記例において、図8に示すステップS98及びS100での処理が第一の署名情報作成手段に対応し、ステップS101での処理が署名情報格納制御手段に対応する。また、特にステップS98での処理が、上記第一の署名情報作成手段におけるファイル読み出し手段に対応し、当該ステップS101での処理は特に

署名情報格納手段における署名情報付加手段に対応する。

【0081】

図8に示すステップS95、S96、S97での処理がクローズ要求に係るファイルに署名情報を付加すべきか否かを判定する署名付加判定手段に対応し、図4に示すステップS24での処理がモード設定手段に対応し、特に、ステップS97での処理がモード判定手段に対応する。

また、図5に示すステップS39及びS41での処理が第二の署名情報作成手段に対応し、ステップS42及びS44での処理が署名一致判定手段に対応し、各ステップS45、S46での処理が判定結果作成手段に対応する。そして、特に、ステップS39での処理がオープンファイル読み出し手段に対応する。

【0082】

図5に示すステップS35、S36、S37での処理が署名チェック判定手段に対応し、図4に示すステップS24での処理がモード設定手段に対応し、特に、図5に示すステップS37での処理がモード判定手段に対応する。

また、更に、図8に示すステップS105での処理が第一の復帰手段に対応し、図5に示すステップS47での処理が第二の復帰手段に対応する。

【0083】

【発明の効果】

以上、説明してきたように、請求項1乃至9、14、16及び17に係る本発明によれば、所望のアプリケーションを立ち上げた状態で、アプリケーションからクローズイベントが発行されると、自動的に当該クローズイベントに係るファイルに対応する署名情報が記憶装置に格納される。従って、ユーザが特に署名情報の作成を意識することなしに、ファイルクローズに係るファイルに対して署名情報が付加されるので、より簡単に署名情報の作成が行えるようになる。

【0084】

また、請求項10乃至13及び15乃至17に係る本発明によれば、所望のアプリケーションを立ち上げた状態で、アプリケーションからオープンイベントが発行されると、自動的に当該オープンイベントに係るファイルに対応する署名情報が作成され、既に当該ファイルに関連付けられた署名情報との一致判定が行わ

れる。従って、ユーザが特に署名情報のチェックを意識することなしに、ファイルオープンに係るファイルのチェックが行われるので、より簡単に署名情報のチェックが行えるようになる。

【図面の簡単な説明】

【図 1】

本発明の実施の一形態に係るファイル処理ユニットが適用されるコンピュータシステムのハードウェア構成を示すブロック図である。

【図 2】

図 1 に示すシステムにおいて、ドライバとファイルシステム（OS）との間でなされるドライバ登録のための処理の手順を示すフローチャートである。

【図 3】

図 1 に示すシステムにおいて、ドライバとファイルシステムとの間でなされる初期処理の手順を示すフローチャートである。

【図 4】

図 1 に示すシステムにおいて、アプリケーションとドライバとの間でなされる認証チェックおよびモード設定についての処理の手順を示すフローチャートである。

【図 5】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるファイルオープンに関する処理の手順を示すフローチャートである。

【図 6】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるリードに関する処理の手順を示すフローチャートである。

【図 7】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるライトに関する処理の手順を示すフローチャートである。

【図 8】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるファイルクローズに関する処理の手順を示すフローチャートである。

【図 9】

モードテーブルの例を示す図である。

【図 10】

フォルダと処理モードとの関係についてのテーブルを示す図である。

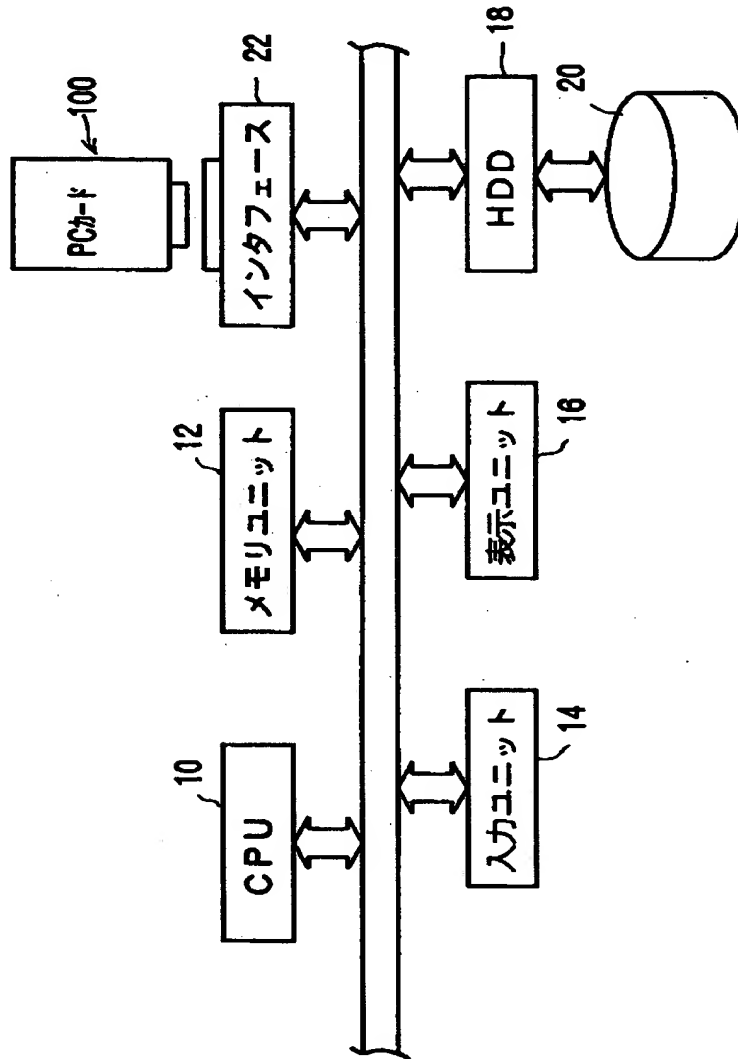
【符号の説明】

- 10 CPU
- 12 メモリユニット
- 14 入力ユニット
- 16 表示ユニット
- 18 ハードディスクドライブユニット
- 20 ハードディスク
- 22 インターフェース回路
- 100 PCカード

【書類名】 図面

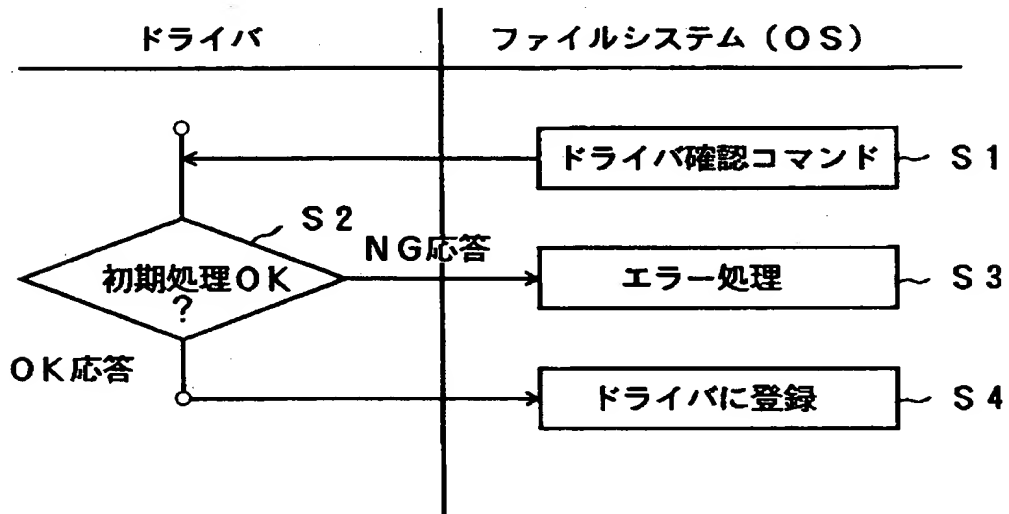
【図 1】

本発明の実施の一形態に係るファイル処理ユニットが適用される  
コンピュータシステムのハードウェア構成を示すブロック図



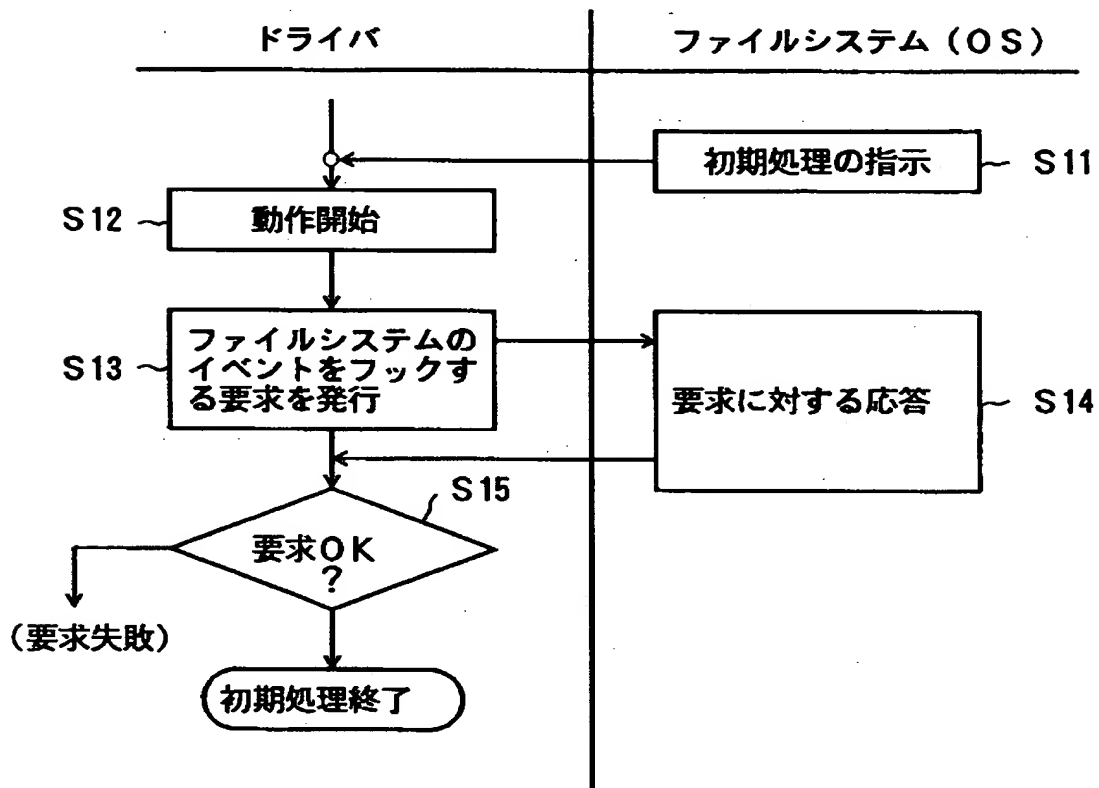
【図 2】

図 1 に示すシステムにおいて、ドライバとファイルシステム（OS）との間でなされるドライバ登録のための処理の手順を示すフローチャート



【図 3】

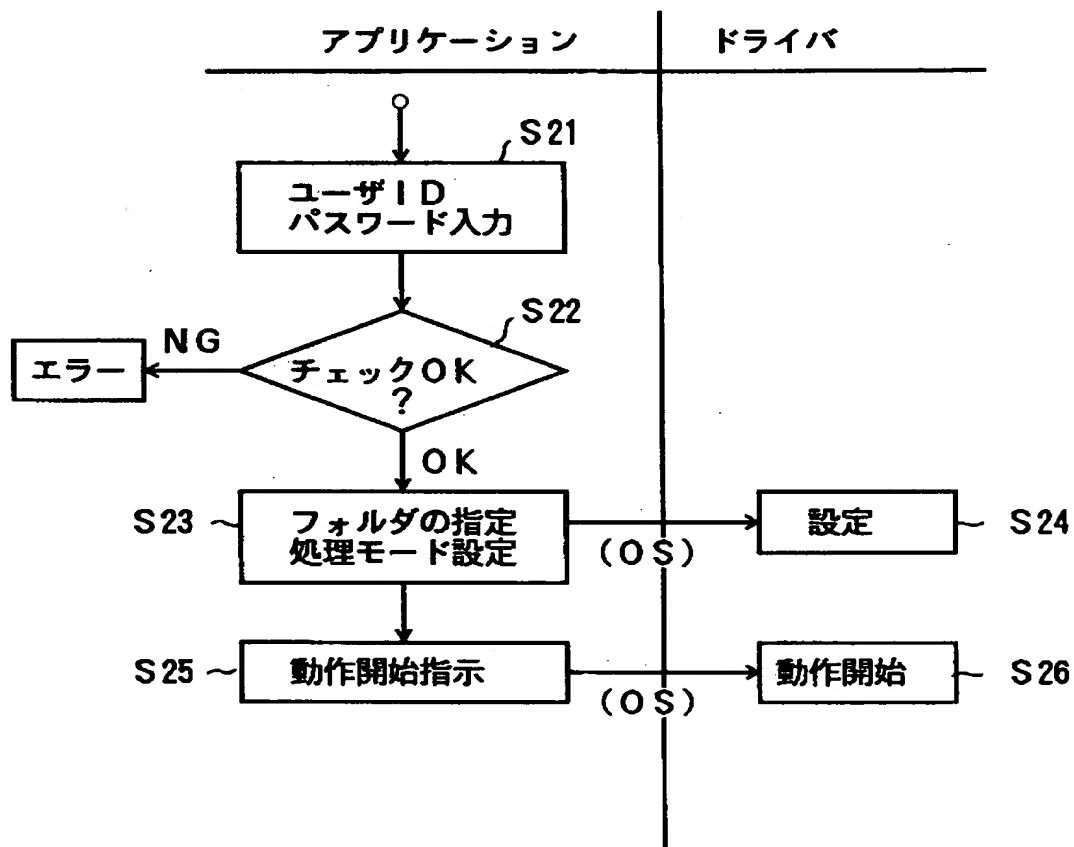
図 1 に示すシステムにおいて、ドライバとファイルシステムとの間でなされる初期処理の手順を示すフローチャート





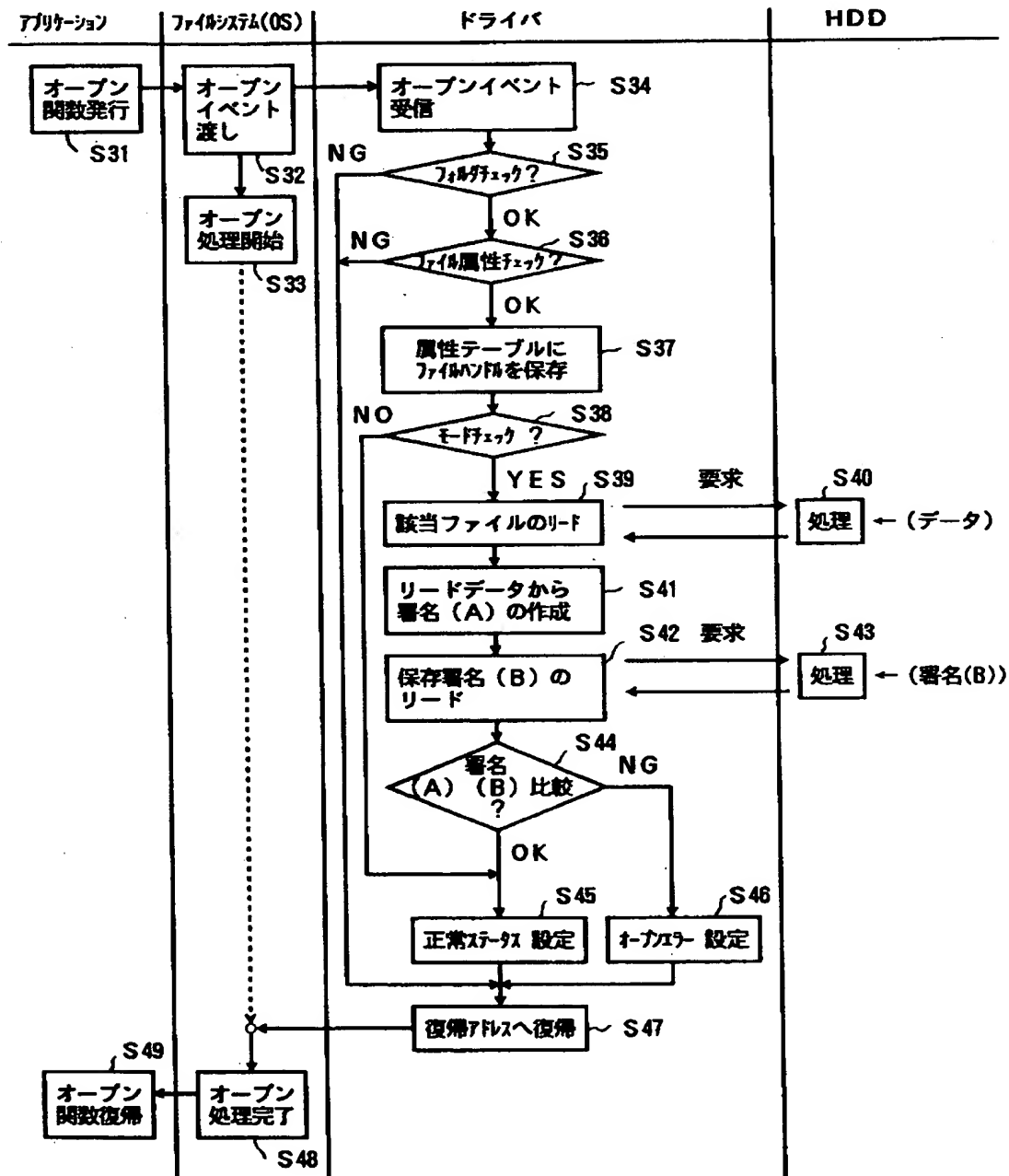
【図 4】

図 1 に示すシステムにおいて、アプリケーションとドライバとの間でなされる認証チェックおよびモード設定についての処理の手順を示すフローチャート



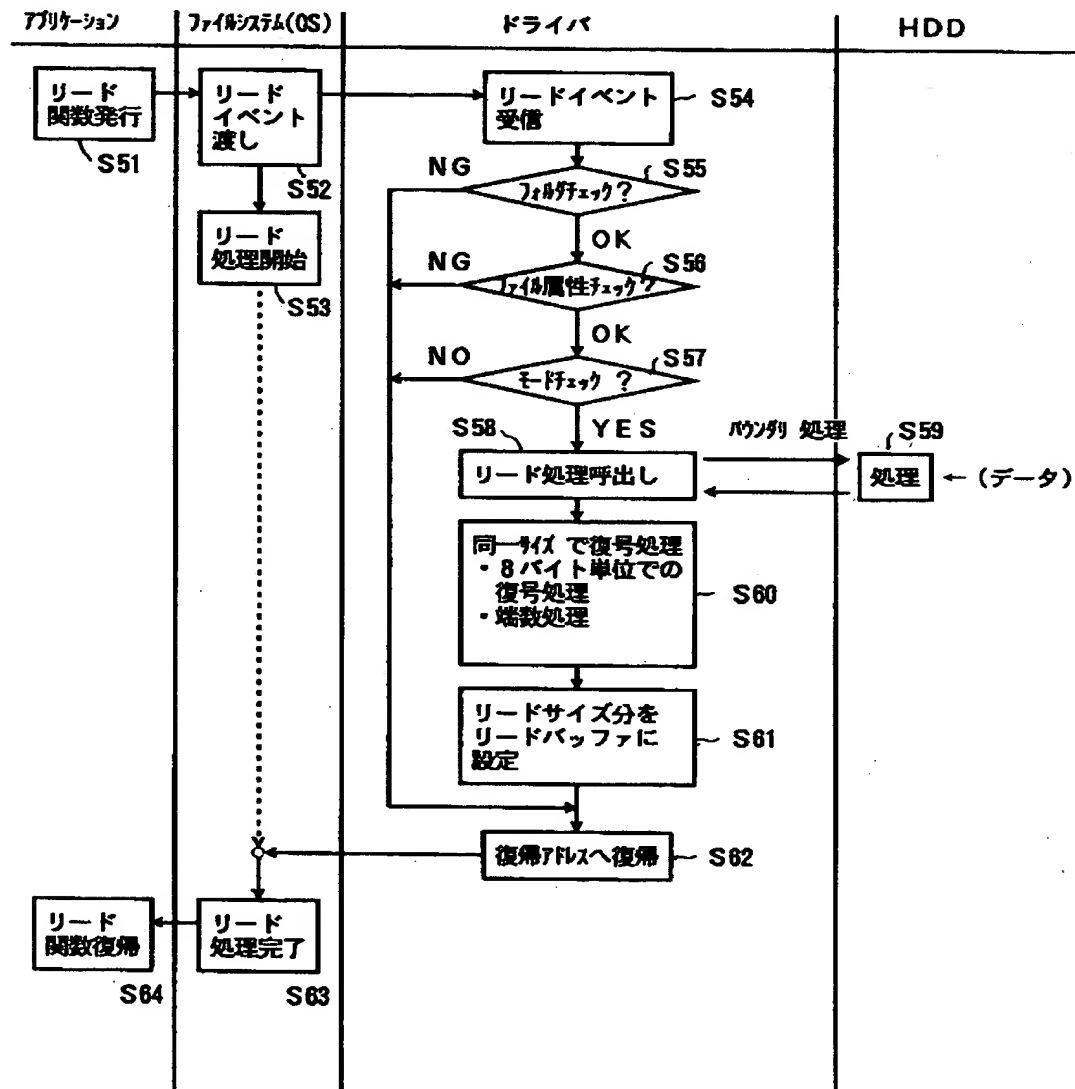
【図 5】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるファイルオープンに関する処理の手順を示すフローチャート



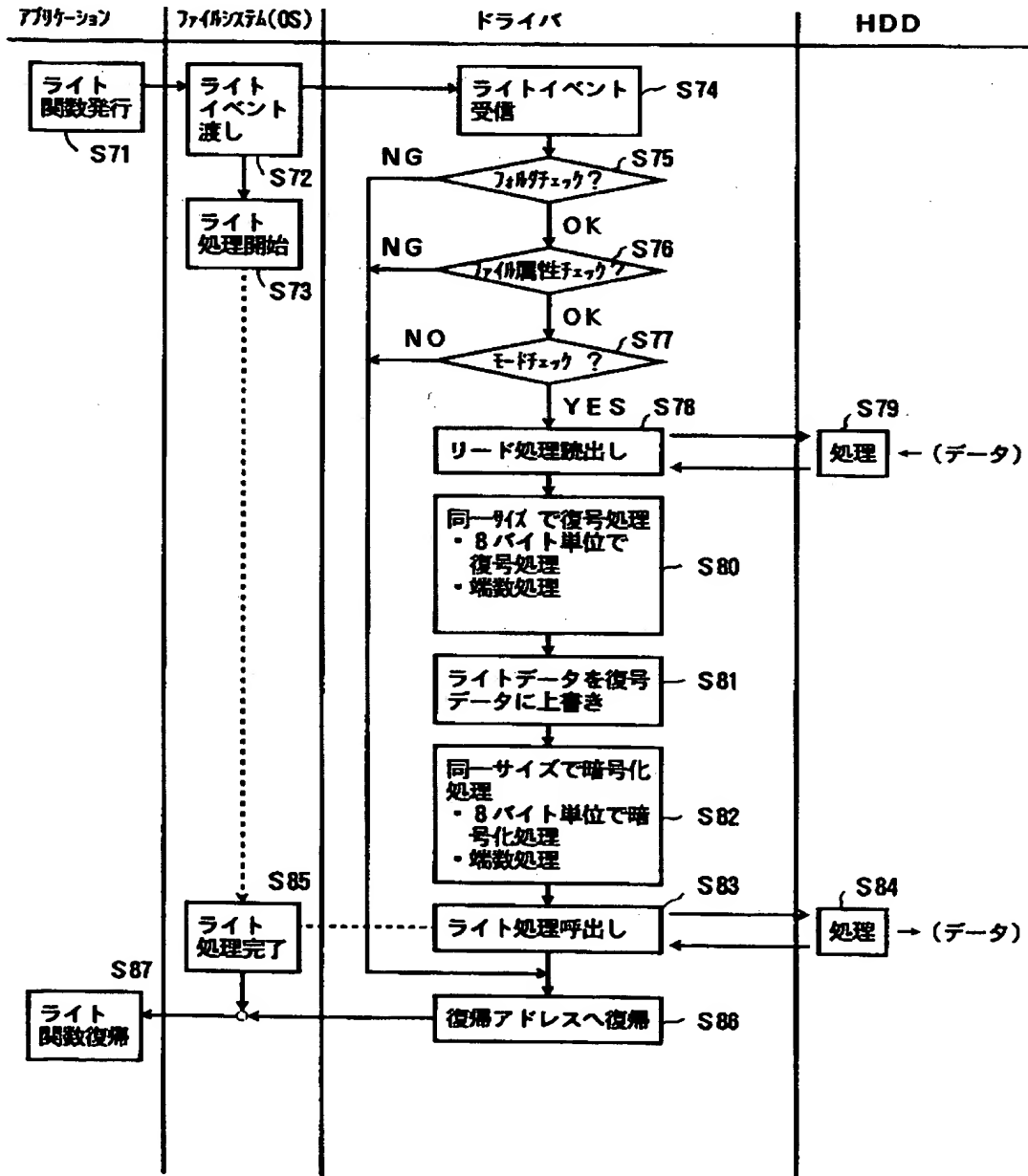
【図 6】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるリードに関する処理の手順を示すフローチャート



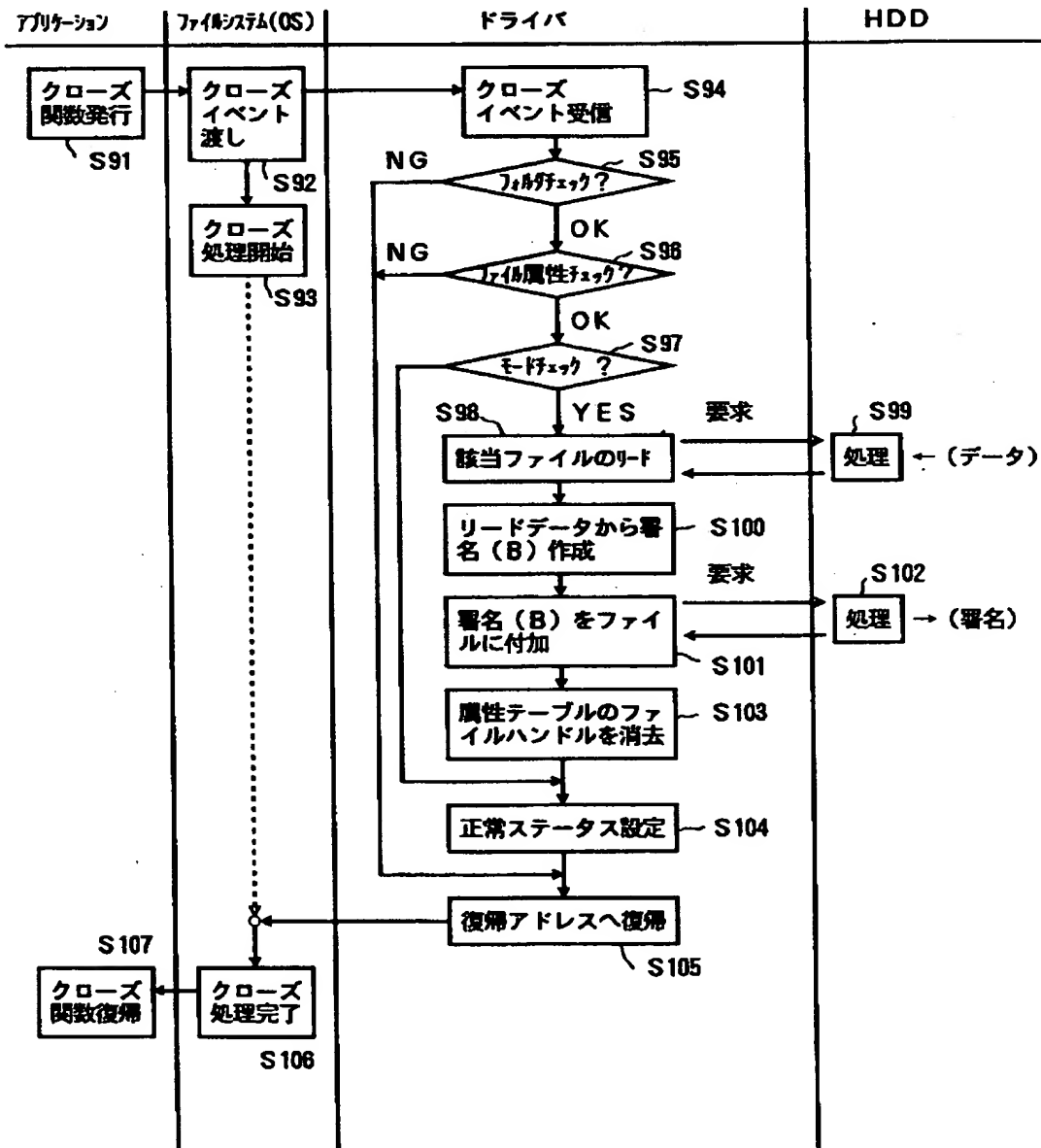
【図 7】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるライトに関する処理の手順を示すフローチャート



【図 8】

図 1 に示すシステムにおいて、アプリケーション、ファイルシステム、ドライバおよびハードディスクドライブユニットの間で行われるファイルクローズに関する処理の手順を示すフローチャート



【図 9】

モードテーブルの例を示す図

オープン時 署名チェック	クローズ時 署名作成	ライト時 暗号化・圧縮	リード時 復号・伸長	モード値 ———
×	×	×	×	0
×	×	×	○	1
×	×	○	×	2
×	×	○	○	3
×	○	×	×	4
×	○	×	○	5
×	○	○	×	6
×	○	○	○	7
○	×	×	×	8
○	×	×	○	9
○	×	○	×	10
○	×	○	○	11
○	○	×	×	12
○	○	×	○	13
○	○	○	×	14
○	○	○	○	15

【図 10】

フォルダと処理モードとの関係についてのテーブルを示す図

モード値	フォルダ
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J
10	K
11	L
12	M
13	N
14	O
15	P

【書類名】            要約書

【要約】

【課題】 所望のアプリケーションにて外部記憶装置に格納されたファイルをアクセスする際に、簡単に署名データの作成、チェックが行えるようなファイル処理システムを提供すること。

【解決手段】 上記課題を解決するため、本発明に係るファイル処理ユニットは、コンピュータシステム内で動作するアプリケーションにて使用されたファイルのクローズ要求が発せられたときに、そのクローズ要求に応答し、当該ファイルのデータを用いて所定の規則に従って第一の署名情報を作成する第一の署名情報作成手段と、該第一の署名情報をクローズ要求に係るファイルと関連付けて記憶装置内に格納する署名情報格納制御手段とを備えるように構成される。

【選択図】            図 8



出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社